Monitoring Citrix Access Gateway

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Citrix Access Gateway™ products are universal SSL VPN appliances providing a secure, always-on, single point-of-access to an organization's applications and data. A comprehensive range of appliances and editions allow Access Gateway to meet the needs of any size organization, from small businesses to the most demanding global enterprises.

The Access Gateway appliance is deployed in an organization's demilitarized zone, and creates a virtual TCP connection with the client computer. Client computers launch the Citrix Secure Access Agent by simply accessing a secure Web URL or using the desktop icon. The Access Gateway then authenticates these credentials with a corporate authentication server and, if the credentials are correct, finishes the handshake with the client PC. Once authenticated, the Secure Access Agent is launched in the client computer, at which all network traffic destined for certain private networks is captured and redirected over the secure tunnel to the Access Gateway.

The error-free functioning of such an appliance is of tremendous significance in environments that span geographies and which support mission-critical applications handling highly sensitive information (like in the case of mobile/VoIP communication). Such environments often have to deal with concurrent access requests from remote users at disparate locations. With a defective Access Gateway, remote traffic could go unscanned and therefore unsecured, exposing the applications and resources to unauthorized usage, or worse, malicious virus attacks.

eG Enterprise offers out-of-the-box two specialized models for monitoring the Citrix Access Gateway – the *Citrix Access Gateway – Windows* model that focuses on the health of the Citrix Access Gateway operating on a Windows platform, and the *Citrix Access Gateway – Linux* model, which is a dedicated model for monitoring the Citrix Access Gateway component operating on Linux.

Using these models, administrators can constantly keep an eye on the operations of the Access Gateway and be proactively alerted of even minor non-conformances, so that the problem is resolved before non-genuine users gain access to critical applications and data.

Chapter 2: How to Monitor Citrix Access Gateway Server Using eG Enterprise?

eG Enterprise is capable of monitoring the Citrix Access Gateway server using an eG external agent on any remote host. The eG external agent periodically polls the SNMP MIB of the Citrix Access Gateway server and fetches metrics related to the performance of the Citrix Access Gateway server. To start monitoring the server, first manage the server using the eG administrative interface. The following section describes how to manage the server.

2.1 Managing the Citrix Access Gateway Server

eG Enterprise offers two specialized models for monitoring the Citrix Access Gateway: the *Citrix Access Gateway – Windows* model and *Citrix Access Gateway – Linux* model. eG Enterprise cannot automatically discover the Citrix Access Gateway server. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Citrix Access Gateway Server component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select a **Component type** based on the platform on which the Citrix Access Gateway operates. The component types offered by the eG Enterprise are provided in the below table:

Operating System	Component Type To be Chosen
Windows	Citrix Access Gateway – Windows
Linux	Citrix Access Gateway – Linux

For instance, choose *Citrix Access Gateway – Linux* as the **Component Type**. Then, click the **Add New Component** button. This will invoke Chapter 2.

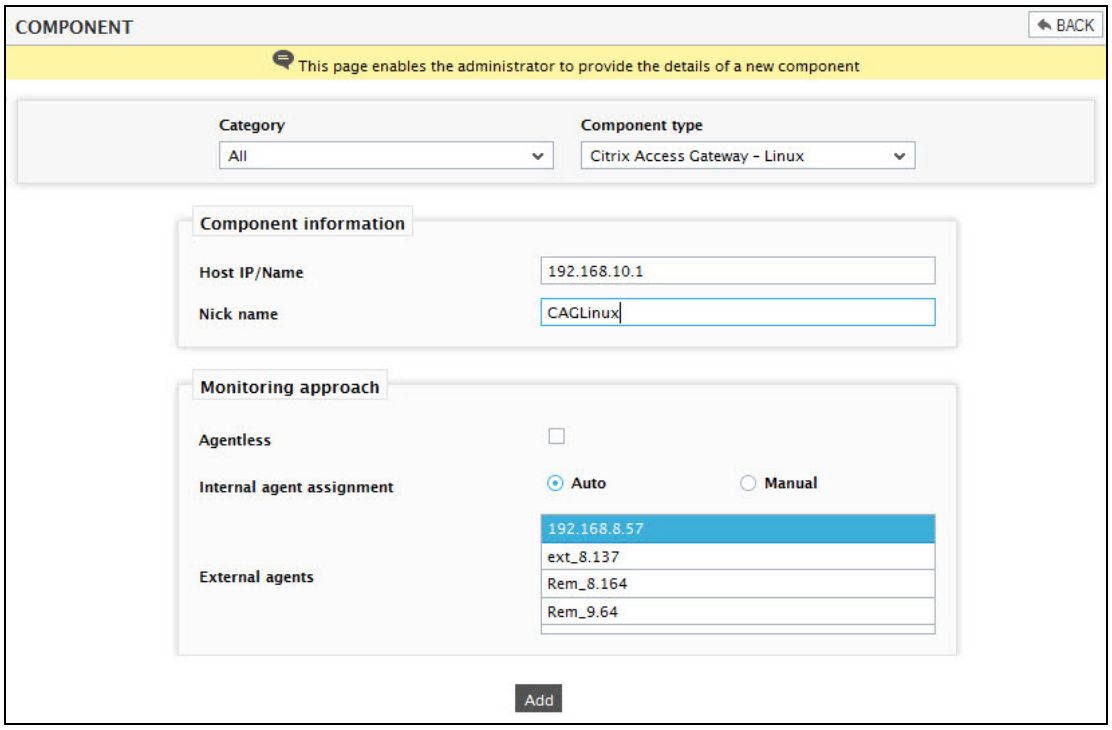

Figure 2.1: Adding the Citrix Access Gateway – Linux component

4. Specify **Host IP/Name** and **Nick name** for the Citrix Access Gateway – Linux component (see Chapter 2). Then, click on the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears.

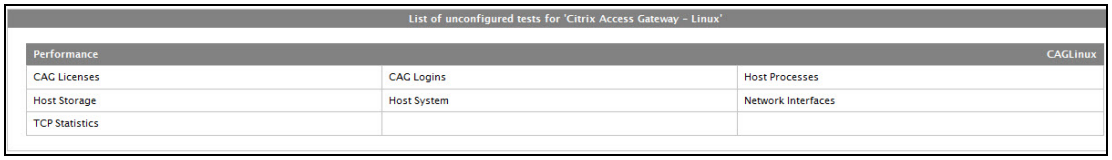

Figure 2.2: List of tests to be configured for Citrix Access Gateway – Linux component

6. Click on the test names to configure. To know how to configure the tests, refer to the **Monitoring the Citrix Access Gateway on Linux** chapter.
7. Finally, signout of the eG administrative interface.
8. The steps discussed above are also applicable for managing the Citrix Access Gateway server operating on a Windows platform. To do this, choose the *Citrix Access Gateway - Windows* as the **Component Type**.

Chapter 3: Monitoring the Citrix Access Gateway on Windows

Figure 3.1 depicts the *Citrix Access Gateway – Windows* model.

Figure 3.1: Layer model of the Citrix Access Gateway

Every layer in the layer model of Figure 3.1 is attached to a wide variety of tests that explore one/more performance aspects of the Access Gateway. With the help of the results reported by these tests, the following performance queries can be easily answered; in the light of these answers, probable issues with the Access Gateway can be instantly detected.

- Is there a processing bottleneck on the Access Gateway?
- What are the type of requests that are being processed, and how quickly is the Access Gateway able to respond to them? Which requests are taking too long?
- Are the context pools adequately sized, or are too many requests waiting for contexts?
- Is the Access Gateway able to create/load sessions quickly upon request, or is there a bottleneck there that requires investigation?
- Is the session cache hit ratio optimal, or do more sessions need to be allocated to the cache?

The sections below discuss the top 3 layers of the layer model only, as the other layers have all been discussed thoroughly in the *Monitoring Unix and Windows Servers* document.

3.1 The .Net Layer

The **.Net** layer tracks the health of the ASP .Net framework on which the Access Gateway operates. Figure 3.2 reveals the tests mapped to this layer.

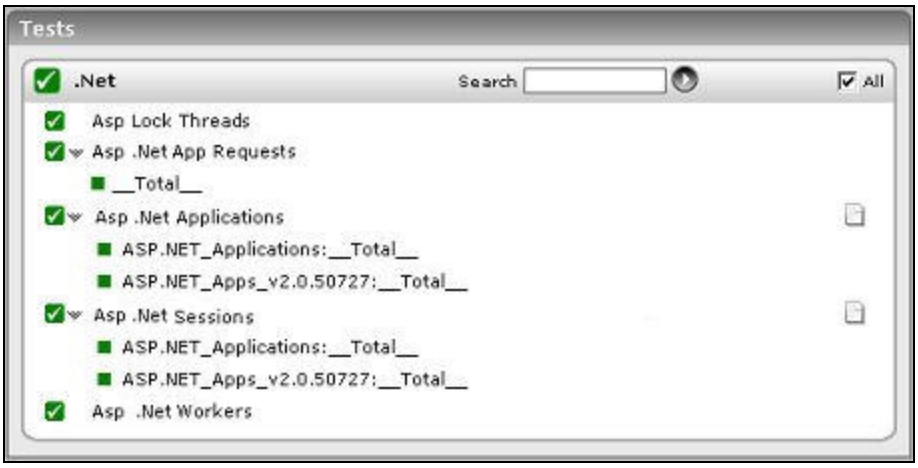

Figure 3.2: The tests mapped to the .Net layer

3.1.1 ASP Lock Threads Test

This test provides information about managed locks and threads that an application uses.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Citrix Access Gateway being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current logical threads	The number of current managed thread objects in the application. This measure maintains the count of both running and	Number	

Measurement	Description	Measurement Unit	Interpretation
	stopped threads.		
Current physical threads	The number of native operating system threads created and owned by the common language runtime to act as underlying threads for managed thread objects. This measure does not include the threads used by the runtime in its internal operations.	Number	
Current recognized threads	The number of threads that are currently recognized by the runtime. These threads are associated with a corresponding managed thread object.	Number	
Contention rate	The rate at which threads in the runtime attempt to acquire a managed lock unsuccessfully.	Rate/Sec	
Current queue length	The total number of threads that are currently waiting to acquire a managed lock in the application.	Number	

3.1.2 ASP .Net App Requests Test

This test monitors how well the application domain handles requests.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every application domain on the ASP .NET framework.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Requests executing	The number of requests currently executing.	Number	This measure is incremented when the HttpRuntime begins to process the request and is decremented after the HttpRuntime finishes the request.
Requests app queue	The number of requests currently in the application request queue.	Number	
Requests not found	The number of requests that did not find the required resource.	Number	
Requests not authorized	The number of request failed due to unauthorized access.	Number	Values greater than 0 indicate that proper authorization has not been provided, or invalid authors are trying to access a particular resource.
Requests timed out	The number of requests timed out.	Number	
Requests succeeded	The rate at which requests succeeded.	Requests/Sec	

3.1.3 ASP .Net Applications Test

This test reports key statistics pertaining to applications deployed on the ASP .NET objects in the Citrix Access Gateway.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every ASP .NET object discovered in the Citrix Access Gateway.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Request rate	Indicates the number of requests executed per second.	Number	This represents the current throughput of the application.
Pipeline instances	Indicates the number of active pipeline instances for the ASP.NET application.	Number	Since only one execution thread can run within a pipeline instance, this number gives the maximum number of concurrent requests that are being processed for a given application. Ideally, the value of this measure should be low.
Number of errors	Indicates the total sum of all errors that occur during the execution of HTTP requests.	Number	This measure should be kept at 0 or a very low value.

3.1.4 ASP .Net Workers Test

This test reports statistics pertaining to the performance of the worker process of the ASP .NET framework of the Citrix Access Gateway.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for Citrix Access Gateway monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Application restarts	The number of application restarts.	Number	In a perfect world, the application domain will and should survive for the life of the process. Even if a single restart occurs, it is a cause for concern because proactive and reactive restarts cause automatic recycling of the worker process. Moreover, restarts warrant recreation of the application domain and recompilation of the pages, both of which consume a lot of time. To investigate the reasons for a restart, check the values set in the processModel configuration.
Applications running	The number of applications currently running.	Number	
Requests current	The number of requests currently handled by the ASP.NET ISAPI. This includes those that are queued , executing, or waiting to be written to the client.	Number	
Request execution time	The number of seconds taken to execute the last request.	Number	In version 1.0 of the framework, the execution time begins when the worker process receives the request, and stop when the ASP.NET ISAPI sends HSE_REQ_DONE_WITH_SESSION

Measurement	Description	Measurement Unit	Interpretation
			to IIS. In version 1.1 of the framework, execution begins when the HttpContext for the request is created, and stop before the response is sent to IIS. The value of this measure should be stable. Any sudden change from the previous recorded values should be notified.
Requests queued	The number of requests currently queued.	Number	When running on IIS 5.0, there is a queue between inetinfo and aspnet_ wp, and there is one queue for each virtual directory. When running on IIS 6.0, there is a queue where requests are posted to the managed ThreadPool from native code, and a queue for each virtual directory. This counter includes requests in all queues. The queue between inetinfo and aspnet_wp is a named pipe through which the request is sent from one process to the other. The number of requests in this queue increases if there is a shortage of available I/O threads in the aspnet_wp process. On IIS 6.0 it increases when there are incoming requests and a shortage of worker threads.
Requests rejected	The number of rejected requests	Number	Requests are rejected when one of the queue limits is exceeded. An excessive value of this measure hence indicates that the worker process is unable to process the requests due to overwhelming load or low memory in the processor.
Requests wait time	The number of seconds that the most recent request spent waiting in the queue, or named pipe that exists between	Secs	

Measurement	Description	Measurement Unit	Interpretation
	inetinfo and aspnet_wp. This does not include any time spent waiting in the application queues.		
Worker processes running	The current number of aspnet_wp worker processes	Number	Every application executing on the .NET server corresponds to a worker process. Sometimes, during active or proactive recycling, a new worker process and the worker process that is being replaced may coexist. Under such circumstances, a single application might have multiple worker processes executing for it. Therefore, if the value of this measure is not the same as that of Applications_running, then it calls for closer examination of the reasons behind the occurrence.
Worker process restarts	The number of aspnet_wp process restarts in the machine	Number	Process restarts are expensive and undesirable. The values of this metric are dependent upon the process model configuration settings, as well as unforeseen access violations, memory leaks, and deadlocks.

3.1.5 ASP .Net Sessions Test

This test monitors the application sessions to the ASP .NET framework of the Citrix Access Gateway.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every application session to the ASP .NET framework.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
SQL connections	Indicates the number of connections to the SQL Server used by session state.	Number	An unusually high value may indicate a sudden increase in sessions to the SQL Server.
State server connections	Indicates the number of connections to the StateServer used by session state.	Number	An unusually high value may indicate a sudden increase in sessions to the StateServer.
Abandoned ASPNet application sessions	Indicates the number of sessions that have been explicitly abandoned during the last measurement period.	Number	
Active ASPNet application sessions	Indicates the currently active sessions.	Number	
Timedout ASPNet application sessions	Indicates the number of sessions that timed out during the last measurement period.	Number	
ASPNet application sessions	Indicates the total number of sessions during the last measurement period.	Number	

3.2 The Web Server Layer

To track the availability, responsiveness, and overall health of the web server component of the Citrix Access Gateway, use the tests associated with this layer.

Figure 3.3: The tests associated with the Web Server layer

Since these tests have already been discussed in the *Monitoring Web Servers* document, let us straight away proceed to the **CAG Service** layer.

3.3 The CAG Service Layer

This layer continuously monitors the requests to the CAG, so as to proactively detect processing bottlenecks (if any), and keeps a check on any unsusual session behavior or session cache usage.

Figure 3.4: The tests associated with the CAG Service layer

3.3.1 CAG Data Layer Test

This test monitors the data layer of the Citrix Access Gateway, and reports the type of requests that are being received by the Access Gateway and how well it processes the requests; in the process, the test reveals processing bottlenecks (if any).

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Citrix Access Gateway being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Contexts in CAG data layer pool	Indicates the number of contexts in the pool.	Number	
Context requests waiting	Indicates the number of context requests waiting on the data layer.	Number	The Citrix Access Gateway embeds SmartAccess capabilities by means of which the Access Gateway can not only grant/deny users access to specific applications/information, but can also determine what the user can do with the information/application so accessed. For example, based on the access device and/or location, organizations can control whether users are allowed to view, print, edit or save information. This is also known as Contextual Access Control. The value of this measure indicates the number of requests that are currently waiting for the Access Gateway to provide context-based access. A high value of this measure implies that context requests are not being processed quickly; this could be owing to a processing bottleneck, and hence warrants further investigation.
Commit rate	Indicates the rate of commits during the last	Commits/Sec	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Update rate	Indicates the rate of updates during the last measurement period.	Updates/Sec	
Delete rate	Indicates the rate of deletes during the last measurement period.	Deletes/Sec	
Insert rate	Indicates the rate of inserts during the last measurement period.	Inserts/Sec	
Context rate	Indicates the rate of contexts during the last measurement period.	Contexts/Sec	
Streams created	Indicates the rate at which streams were created during the last measurement period.	Creates/Sec	The application streaming feature simplifies application deployment to end users. With the application streaming feature, you can install and configure an application on one file server and deliver it to any desktop or server on demand. While publishing a streamed application for access by end users, you also need to configure the Access Gateway to allow such a user access. These measures help administrators gauge how well the Access Gateway handles user requests for published applications.
Read streams created	Indicates the rate at which read streams were created.	Creates/Sec	
Write streams created	Indicates the rate at which write streams were created.	Creates/Sec	
Stream data read rate	Indicates the rate at which stream data was read.	KB/Sec	
Stream data write rate	Indicates the rate at which stream data was written.	KB/Sec	

3.3.2 CAG Sessions Test

This test monitors the sessions to the Citrix Access Gateway, exposes delays or other abnormalities in session creation/validation/loading, and stark inefficiencies (if any) in session cache utilization.

Target of the test : A Citrix Access Gateway

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Citrix Access Gateway being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specific host is listening.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CAG sessions started	Indicates the rate at which sessions were created on the Citrix Access Gateway.	Creates/Sec	
CAG sessions updated	Indicates the rate at which the sessions were updated during the last measurement period.	Updates/Sec	
CAG sessions validated	Indicates the rate at which sessions were validated during the last measurement period.	Validates/Sec	
CAG sessions loaded	Indicates the rate at which sessions were loaded during the last measurement period.	Updates/Sec	
CAG sessions saved	Indicates the rate at which sessions were saved during the last measurement period.	Saves/Sec	
CAG sessions deleted	Indicates the rate at which sessions were deleted during the last measurement period.	Deletes/Sec	
CAG session cache	Indicates the rate at which	Hits/Sec	Ideally, this value should be high. A

Measurement	Description	Measurement Unit	Interpretation
hits	session requests were serviced by the session-cache during the last measurement period.		low value indicates that session requests are often fulfilled by direct disk accesses, thus increasing the processing overheads. You might want to increase the session cache size, if the situation persists.
CAG session cache misses	Indicates the rate at which the session-cache could not service session requests during the last measurement period.	Misses/Sec	Ideally, this value should be low. A high value indicates that session requests are often fulfilled by direct disk accesses, thus increasing the processing overheads. You might want to increase the session cache size, if the situation persists.

Chapter 4: Monitoring the Citrix Access Gateway on Linux

Figure 4.1 depicts the *Citrix Access Gateway - Linux* monitoring model that eG Enterprise offers.

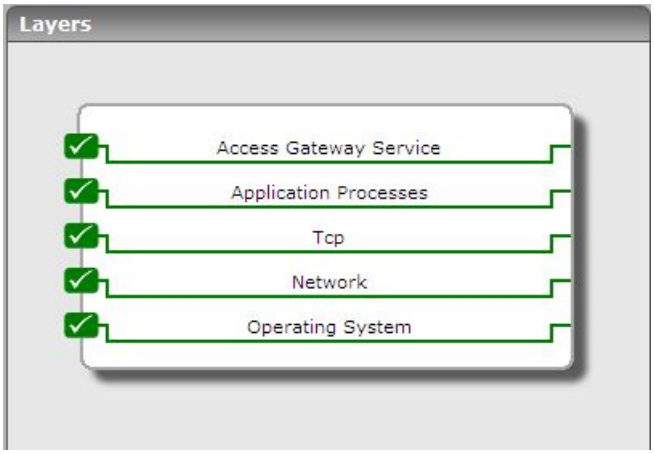

Figure 4.1: The layer model of the Citrix Access Gateway on Linux

Each layer is mapped to tests that periodically poll the SNMP MIB of the Citrix Access Gateway to retrieve useful performance statistics. These statistics reveal the following:

- Have any login attempts to the CAG failed?
- Have any administrative login attempts failed?
- Has the connection pool been utilized optimally or have too many connections been used already?

4.1 The Operating System Layer

Using the tests mapped to this layer, administrators can track the usage of every storage area of the CAG and instantly identify the areas that are running out of storage space. In addition, the layer also monitors the number of processes running on the CAG and the number of users currently connected to it.

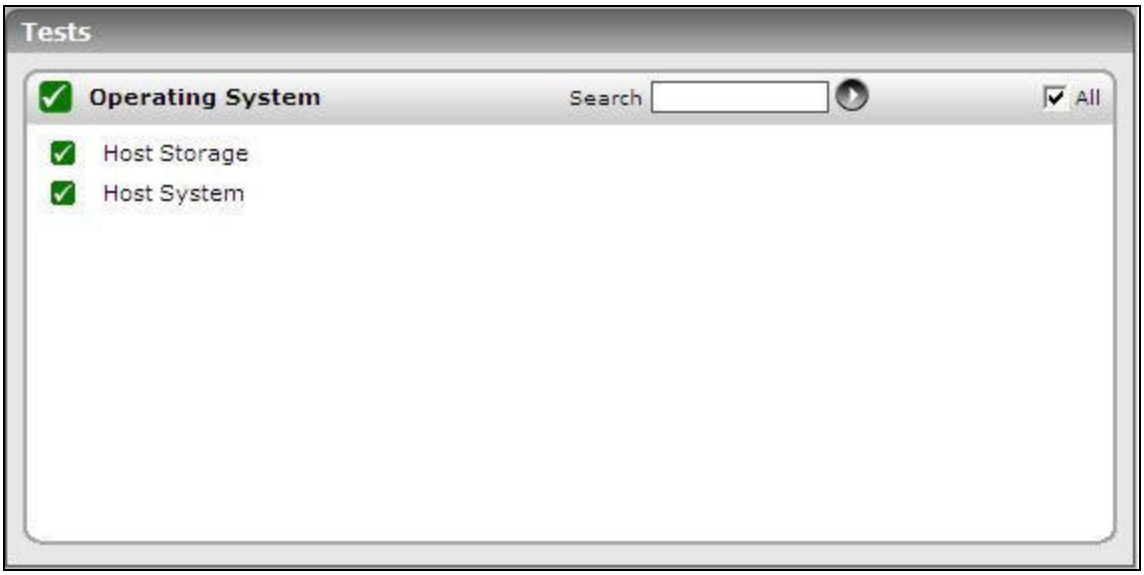

Figure 4.2: The tests mapped to the Operating System layer

4.1.1 Host Storage Test

This test auto-discovers all the storage areas of the CAG and tracks the usage of each of these areas.

Target of the test : CAG on Linux

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every storage area on the server being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Storage size	Represents the total size of a storage area associated with a server.	GB	
Usage of storage area	This metric denotes the percentage capacity of a storage area that is currently allocated.	Percent	A value close to 100% denotes a storage area that is highly used.
Free space on storage area	This metric denotes the amount of storage of a storage area that is currently available for use.	GB	
Allocation failures on storage area	The number of requests for storage represented by this entity that could not be honored in the last measurement period because there was not	Number	Ideally, there should be no allocation failures.

Measurement	Description	Measurement Unit	Interpretation
	enough storage available to service application requests		

4.1.2 Host System Test

This test monitors the number of users accessing the CAG device and the processes executing on the device.

Target of the test : CAG on Linux

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each server being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.

Parameter	Description
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Parameter	Description
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current users	The current number of users logged in to the server being monitored.	Number	
Current processes	The current number of processes executing on the server being monitored.	Number	

4.1.3 The Network Layer

Monitor the availability and responsiveness of the CAG over the network, and also measure the bandwidth usage of each network interface supported by the CAG, with the help of the tests mapped to this layer.

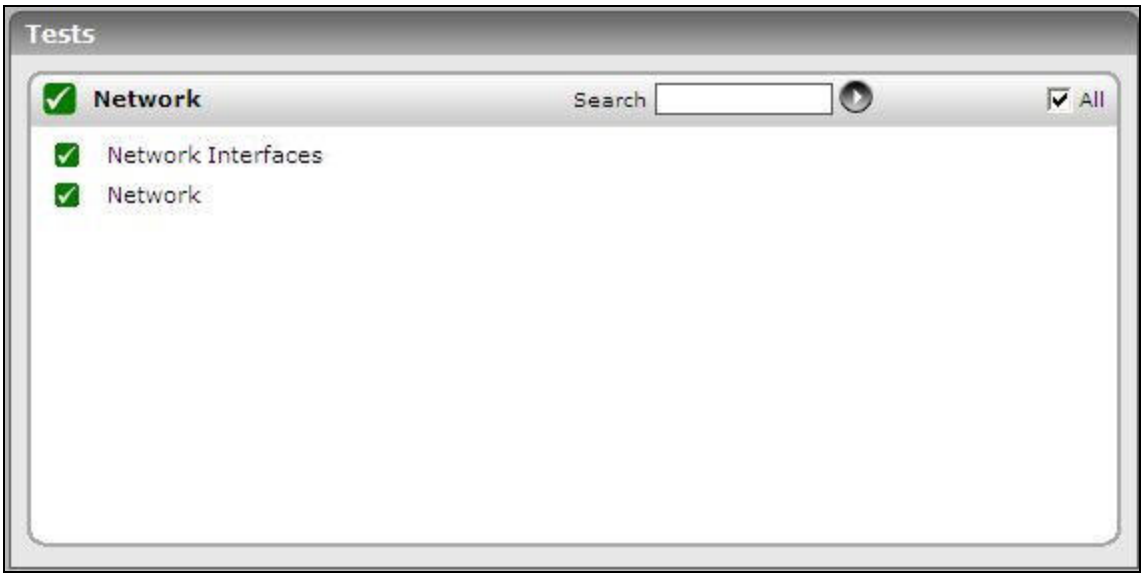

Figure 4.3: The tests mapped to the Network layer

Since these tests have already been discussed in the *Monitoring Unix and Windows Servers* document, let us proceed to the next layer.

4.2 The Tcp Layer

This layer measures the health of TCP connections to and from the CAG and also tracks TCP retransmissions.

Figure 4.4: The test mapped to the Tcp layer

Refer to the *Monitoring Unix and Windows Servers* document for the detaild discussion on the TCP test.

4.3 The Application Processes Layer

You can track the availability and resource usage of critical processes executing on the CAG using the test mapped to this layer.

Figure 4.5: The test mapped to the Application Processes layer

4.3.1 Host Processes Test

This test monitors the specific processes executing on CAG and reports the resource usage of the processes.

Target of the test : CAG on Linux

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every configured process pattern.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameters	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameters	Description
	selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Processes running	The number of processes currently executing on the server that match the pattern specified as parameter.	Number	This value indicates if too many or too few processes corresponding to an application are executing on the host.
Memory utilization	The total memory usage of all processes executing on the server that match the pattern specified as parameter. The memory usage is specified as a percentage of the total memory available on the server.	Percent	A very high value could indicate that processes corresponding to the specified pattern are consuming excessive memory resources.
Memory size	The total memory usage(in	MB	A sudden increase in memory

Measurement	Description	Measurement Unit	Interpretation
	MB) of all processes executing on the server that match the pattern specified as parameter.		utilization for a process(es) may be indicative of memory leaks in the application.
CPU utilization	The total CPU utilization of all processes executing on the server that match the configured process pattern.	Percent	A high value could signify a CPU bottleneck. The CPU utilization may be high because a few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource. Check the currently running processes to see the exact cause of the problem.

4.4 The Access Gateway Service Layer

The tests mapped to this layer monitors the efficiency with which the CAG performs its core functions, which include:

- Login authentication
- Managing client connections

Figure 4.6: The tests mapped to the Access Gateway Service layer

4.4.1 CAG Licenses Test

This test monitors how well the CAG manages connections to the Citrix server.

Target of the test : CAG on Linux

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the CAG monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total licenses	Indicates the maximum	Number	

Measurement	Description	Measurement Unit	Interpretation
installed on the Access Gateway	number of client connections.		
Licenses in use	Indicates the number of connections currently used.	Number	
Disabled licenses	Indicates the number of connections currently disabled.	Number	
Licenses available for use	Indicates the number of connections currently unused.	Number	
Available licenses percent	Indicates the percentage of unused connections.	Percent	Ideally, this value should be high. A low value indicates that too many connections are currently in use, and that the pool might not have enough connections to support subsequent connection requests. This can severely affect the user experience with the CAG.

4.4.2 CAG LoginsTest

This test tracks the user logins to CAG, and captures failed login attempts.

Target of the test : CAG on Linux

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the CAG monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameters	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

Parameters	Description
	default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total logins	Indicates the number of logins during the last measurement period.	Number	
Client user logins	Indicates the number of successful client logins to the CAG during the last measurement period.	Number	
Failed logins	Indicates the number of client logins that failed during the last measurement period.	Number	Ideally, this value should be 0.

Measurement	Description	Measurement Unit	Interpretation
Admin user logins	Indicates the number of successful admin user logins during the last measurement period.	Number	
Failed admin user logins	Indicates the number of failed admin user logins during the last measurement period.	Percent	Ideally, this value should be 0.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.